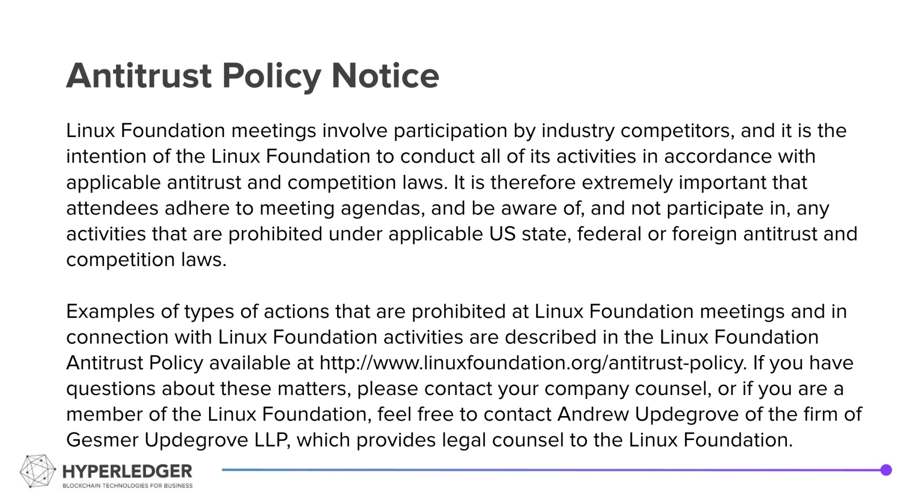
2021-03-23: Indy DID Method Specification Call

Summary

- Identifiers with naming for non-NYM ledger objects
- Serialization formats - use JSON?
- If there is time: A "close to finished" DID Method Specification?

Recording from the call:

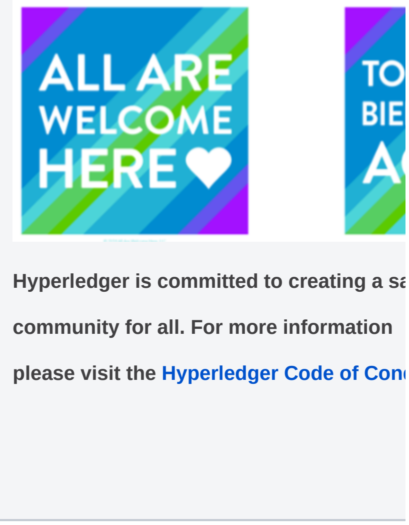


Antitrust Policy Notice

Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS



Hyperledger is committed to creating a sa

community for all. For more information

please visit the Hyperledger Code of Con

Welcome and Introductions

Announcements

Attendees

- Stephen Curran

Collaboration Channels

- Current hackmd document
- indy-did-method on RocketChat - https://chat.hyperledger.org/channel/indy-did-method
- indy-did-method repo: ~~ReSpec vs.~~ SpecUp

Agreed Upon:

- See HackMD Document for most of what we have discussed

Online Discussion (from RocketChat this week)

- Serialization formats

This Week's Discussion:

- Note: Work from Gimly (Jack Tanner) on "DID verifiable conditions" – e.g. "N of M signatures to update a DID" – https://github.com/Gimly-Blockchain/verifiable-conditions
- Other Indy Ledger Objects as DIDs (e.g. schema, etc):
    - Schema: "F72i3Y3Q4i466efjYJYCHM:2:npdb:4.3.4" (<nym_id>:<object version>:<name>:<tag>)
        - Do we want to allow the embedded reference to the "owner" of this item to be on another ledger? My guess – no.
        - How do we get a namespace into that? I think changing the <nym_id> to a <did> would resolve it.
            - That would make it look like a DID, even though the DID is just a component.
            - Do we auto-detect the "type of DID"?
            - Presumably if "?resource=true" returns the ledger object, but what if that query parameter is left off? Do we just return the DIDDoc of the DID?
    - CLAIM_DEF: "5nDyJVP1NrcPAttP3xwMB9:3:CL:56495:npdb" (<nym_id>:<object version>:<signature_scheme>:<schema_txn>:<tag>)

        - Note how the schema is referenced in the CLAIM_DEF identifier – as a transaction ID.
    - REVOC_REG_DEF: "5nDyJVP1NrcPAttP3xwMB9:4:5nDyJVP1NrcPAttP3xwMB9:3:CL:56495:npdb:CL_ACCUM:TAG1" (<nym_id>:<ver>:<cd_nym_id>:<ver>:<sig>:<seqno>:<?>:<?>:<tag>)
    - REVOC_REG_ENTRY: "5:5nDyJVP1NrcPAttP3xwMB9:4:5nDyJVP1NrcPAttP3xwMB9:3:CL:56495:npdb:CL_ACCUM:TAG1" (<?>:<nym_id>:<ver>:<cd_nym_id>:<ver>:<sig>:<seqno>:<?>:<?>:<tag>)

Questions:

- How can we change those to enable naming?
    - Where it matters: in the credential, in the proof request and in the proof.
    - Idea (above): change the "<nym_id>" to "<did>" in the identifier
- How much cross-ledger referencing do we allow?
    - My position: Allowing the schema to be on any ledger is the only cross-register use case that reallly makes sense.
        - Why? We want schema objects shared, so ideally, there is one and all others reference that instance.
        - Clearly the NYM_ID has to be local to enable the writing of any related object, as it is used to identify the writer.
        - Requiring that a REVOC_REGDEF/REVOC_REG_ENTRY be on the same ledger as the CLAIM_DEF is not an onerous constraint
- Presumably, that means we need to update the embedded SCHEMA ID in the CLAIM_DEF ID to be a full schema ID (<did>:<version>:<schema>:<tag>)
    - Could we use <did>:<seqno> to reference the schema? Could we use just <seqno> to mean "on this ledger"?

- The "close-to-finished" DID Method Spec – please review
    - Perhaps not close to finished – doesn't talk about other objects yet – the conversation above
    - At risk – DNR/DND

Future Discussions:

- Include in document that DIDDocs are JSON-LD
    - Three serialization formats in the DID Core spec – let's go with 1 to reduce interop and implementation effort.
    - Daniel Hardmanwants to discuss this further, so that we consider JSON.
- DNR and DND discussions
    - To find networks we will require at least the first and perhaps the second of these approaches, while the rest are suggested:
        - Config files for one or more known networks
        - A mechanism for a ledger operator to register discovery information for other ledgers (aka "human gossip")
            - A DID/DIDDoc on a ledger will contain cross-registry information
            - A mechanism is needed for finding the DID(s) that contain the registrations – ideas have been put forward - a DID Name Directory (DND) is the likely approach.
            - Document about the DND and DNR records
        - Decentralized registries based on verifiable credentials
        - Other registry mechanisms, such as the DDNR proposal
        - The DID Method Spec will include a reference to a repo (likely) "indy-did-networks" within Hyperledger that will be a lightly managed, structured repository of folders per Indy network with at least the config file(s) for the networks. Use of the repo is voluntary, but provides a convenient way for networks to publish information about the network. Maintainers will be selected from the community and should exhibit a light hand in accepting PRs, being concerned mainly with structure of the data (not content) and that contributors are not being malicious about updating the information of other network operators. The Hyperledger governance structure may be used for disputes as appropriate. This is not a replacement for the Governance that a specific network should implement.